Brian Sandoval
Governor

Barbara Smith Campbell
Chairwoman

Jon M. Hager
Executive Director

Silver State Health Insurance Exchange

2310 S. Carson Street, Suite 2, Carson City, NV 89701 • T: 775-687-9939 F: 775-687-9932
exchange.nv.gov

DELIVERABLE INFORMATION	
TYPE OF DELIVERABLE:	☑ Payable ☐ Non-Payable
CONTRACTOR:	Xerox
PROJECT NAME:	BOS
DELIVERABLE #:	5.5.7.16
DELIVERABLE TITLE:	Configuration Management Plan
DUE DATE PER CONTRACT:	N/A

DELIVERABLE SUBMISSION AND REVIEW HISTORY			
Deliverable Submission #	**Date and Time Received From Contractor**	**Date Returned to Contractor**	**Notes / Comments**
1	04/25/13		
2		05/03/13	Configuration Management Plan returned with edits
3	05/13/13		
4		05/16/13	State Accepts Configuration Management Plan

STATE FINAL APPROVAL AND ACCEPTANCE OF DELIVERABLE		
APPROVED BY:	**SIGNATURE**	**DATE**
Agency IT Lead:		
Agency Project Manager:	Jon. DeLaurie	5/17/13

Distribution	Original: Project Office - Agency Contract Monitor
	Copies: Contractor

Exchange Documentation and Finance Use

☐	Scan Deliverable Acceptance Form & Deliverable Document into single document (naming convention is deliverable # and document name)
☐	E-mail above scan to Xerox Team (Bill DeLange-bill.delange@xerox.com and Michelle Lashley- michelle.lashley@xerox.com)
☐	Validate Cost; Post to Contract Log
☐	RCVD Invoice and Process Payment (contact: Karen Robinson-karen.robinson@xerox.com)
☐	Update online CALT and Exchange CALT File (If Applicable)

23. Configuration Management Plan

23.1 Introduction

The purpose of this Configuration Management Plan (CM Plan) is to:

- Identify and document the functional and physical characteristics of any product, component, result, or service.
- Control any changes to such characteristics.
- Record and report each change and its implementation status.
- Support the audit of the products, results, services, or components to verify conformance to requirements.

Configuration management (CM) activities for the Business Operation System (BOS) will apply to both the software and hardware controlled configurations components. This CM Plan is one of several project plans that support the overall Project Management Plan (PMP) structure for the BOS solution. This plan will be used in conjunction with other core plans, including the release management plan and change management plan, to manage the integrity of BOS software and hardware. The CM Plan defines the processes used to identify and manage each Configuration Item (CI) controlled within the BOS. CM practices for documents are excluded from this plan and will be controlled under the projects change management processes.

23.1.1 Purpose

The purpose of CM is to:

- Identify and document the functional and physical characteristics of the BOS systems and its associated components
- Control any changes to such characteristics
- Record and report each change and its implementation status
- Support the audit of the BOS system components to verify conformance to requirements

CM allows the BOS to be developed or modified in a consistent and verifiable manner. CM minimizes the confusion and error that can be caused by different or multiple versions of a CI.

23.1.2 Scope and Approach

The BOS is comprised of several systems including the Exchange Web Portal, Call Center IVR-ININ, Data Warehouse, COGNOS reporting inclusive of the foundation architecture and external interfaces.

CM processes will be applied to these systems in conjunction with other project management processes such as release management and change management as the BOS is being developed for its initial deployment and for ongoing maintenance.

This CM Plan applies to staff assigned to the implementation and support of the BOS systems during its development, implementation, and ongoing operations. The CM processes are in place to effectively manage components of the BOS that are under configuration in a common verifiable manner. CM does not apply to changes to documents, business processes or methodology. Management of changes to documents, processes or methodology will be applied from activities from the change management plan. CM as defined in this plan applies to BOS system changes as it relates to software and hardware for the BOS systems.

The appropriate degree of formality in the execution of any systems engineering process activity is determined by:

- The need for communication of what is being done (across members of a project team, across organizations, or over time to support future activities)
- The level of uncertainty
- The degree of complexity
- The consequences to human welfare

CIs are assigned a level of configuration as either full or limited configuration. Full configuration means they have a rule or other document that defines what, when, where, why and how they are configured. Limited configuration means they have an owner who is responsible for the configuration of the item.

The BOS system is comprised of systems, support staff, and processes that deliver a service of a Patient Protection and Affordable Care Act (PPACA) compliant State Based Exchange. Distinct deliverables to be delivered at project close will be defined and updated as we progress through the development and implementation of the BOS system. These deliverables may be comprised of project closure reports, disposition plans of data or project document artifacts however, would exclude system code, physical software or hardware.

23.1.3 Constraints and Assumptions

- The BOS systems and CIs may be affected by the external system changes e.g. NOMADS, HCR EE.
- The BOS teams will commence CM activities within the constraints of this plan and adjust or further implement practices once its approval has been received.

23.1.4 Risks and Response

CM risks that are identified will be managed as defined in the risk management plan.

In the absence of CM, or where it is ineffectual, there may be system failures due to incorrect implementation of changes or updates; schedule delays, potential unplanned costs; operational delays due to mismatches with support assets; maintenance problems, down-time, and increased maintenance cost due to inconsistencies between systems, software or hardware.

23.1.5 Key Terms

The following is a list of terms and acronyms used in the CM Plan.

Table 23.1.5-1 : Configuration Management Terms and Acronyms

#	Term/Acronym	Definition
1.	BMC	BMC FootPrints is the CMS software, which will be the point of authority for all request for changes and change requests
2.	BOS	Business Operation System
3.	CCB	Change Control Board - A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes
4.	CCD	Configuration Control Decision
5.	CCM	Change Control Management
6.	CI	Configuration Item – An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process (IEEE Std. 610.12-1990)
7.	CM	Configuration Management – A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements (IEEE Std. 610.12-1990)
8.	CMDB	Configuration Management Database
9.	CM Plan	Configuration Management Plan
10.	CMS	Configuration Management System
11.	COGNOS	The BOS reporting tool
12.	CR	Change Request
13.	CSA	Configuration Status Accounting
14.	DCIL	Document Configuration Items List

#	Term/Acronym	Definition
15.	DOORS	IBM DOORs is the requirements traceability database that will be used by the Exchange teams to track requirements and produce an initial, subsequent requirements traceability matrices, and subsequent change requests
16.	DHL	Definitive Hardware Library - A secure Information Technology repository or list of controlled CI's hardware configurations and baseline software are stored and protected. In addition to a list for configuration and baseline software, the DHL can also in part be a storage location for hardware not currently in use in a controlled environment
17.	DWSS	Department Welfare & Supportive Services
18.	DML	Definitive Media Library - A secure Information Technology repository, in which an environment's definitive, authorized versions of software media are stored and protected. An example of a DML is a Network Share controlled by Configuration Management
19.	HCR-EE	Health Care Reform Eligibility Engine
20.	IBM	International Business Machine Corporation
21.	IEEE	Institute of Electrical and Electronics Engineers
22.	IVR-ININ	Interactive Voice Response- Interactive Intelligence
23.	LLC	Limited Liability Company
24.	NOMADS	Nevada Operations of Multi-. Automated Data Systems
25.	PMO	Project Management Office
26.	PMP	Project Management Plan
27.	RM	Release Management
28.	RFP	Request for Proposal
29.	SLA	Service Level Agreement
30.	SCM	Software Configuration Management – The discipline of configuration management specifically applied to software configuration items
31.	SIT	System Integration Testing
32.	TBD	To be Determined
33.	TFS	Team Foundation Server

#	Term/Acronym	Definition
34.	UAT	User Acceptance Test
35.	UCM	Unified Change Management (UCM) is the object-oriented realization of ClearCase, a set of software tools typically supporting the process area software configuration management

23.1.6 References

The following items serve as references and sources for development of the CM Plan:

- Contract for Services of Independent Contractor; A Contract Between the State of Nevada Acting by and Through Its Silver State Health Insurance Exchange and Xerox State Healthcare LLC)
    - Attachment CC: Deliverable Payment Schedule
    - Attachment DD: Requirements Matrix

- RFP 2023 (Silver State Health Ins Exchange) FINAL.docx (Attachment EE and FF as amended by Attachment AA)
    - Attachment O - RFP 2023 (Silver State Health Ins Exchange) FINAL.docx (Attachment O of RFP 2023 as included in Attachment FF, Contractor's Response and Amended by Attachment AA, Negotiated Items)
    - Section 4 – System Requirements

- IEEE Std 828 - 2012 IEEE Standard for Configuration Management in Systems and Engineering

23.2 CM Overview and Contents

The CM Team is responsible for planning the project's configuration activities and the management of its CIs during the Initial Deployment and Ongoing Maintenance phases. The project's CM activities are coordinated with Change Control and Release Management processes to implement BOS changes in a structured, repeatable manner. This plan provides a framework for managing CIs in a formal and systematic approach.

The CM Team is responsible for verifying that project team members are aware of the CM systems (e.g., Microsoft Team Foundation Server, IBM Rational ClearCase, and BMC Footprints) and applicable CM best practices. The CM Group is also responsible for the project team's adherence to standards and processes including obtaining appropriate approvals.

The following sections will describe four (4) topics to address the project's plan for CM:

- The Xerox Teams which CM will apply to (e.g. the Project Management Office (PMO), Release Management (RM) or Change Management teams)

- CM responsibilities of the Xerox Teams which will adhere to the CM Plan

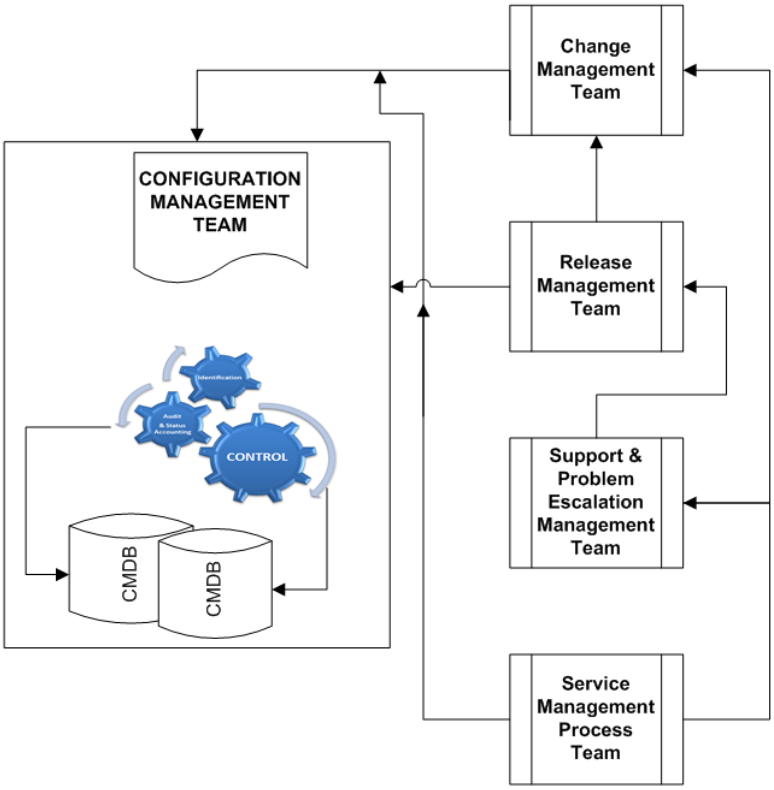
- CM policies or directives that apply to the BOS solution

- CM consisting of:
    - CM Activities
    - CM Schedules
    - CM Resources
    - CM Plan Maintenance

23.3 CM Teams

The following diagram displays the management processes that work in conjunction with the CM Plan. The teams as described in each plan will be involved in receiving, assessing, executing, monitoring and controlling a change.

Figure 23.3-1 : Management Plan Relationships



23.4 Policies and Directives

The BOS will apply CM activities as described, and will be in alignment with each BOS systems policies and directives. This plan will adhere to changes to configuration management of its systems, in the event of policy or directive changes.

23.5 Configuration Management

The following sections describe CM activities, schedules, resources and maintenance.

23.5.1 CM Activities

The following section describes the detailed activities for CM. CM activities include all functions and tasks required in managing the CIs of the BOS environment as specified in the scope of this plan. Both technical and managerial CM activities will be identified and controlled through the following CM processes:

- Configuration Identification
- Configuration Control
- Configuration Status Accounting
- Configuration Audits and Reviews
- Subcontractor/Vendor Control
- Release Management and Delivery

23.5.1.1 Configuration Identification

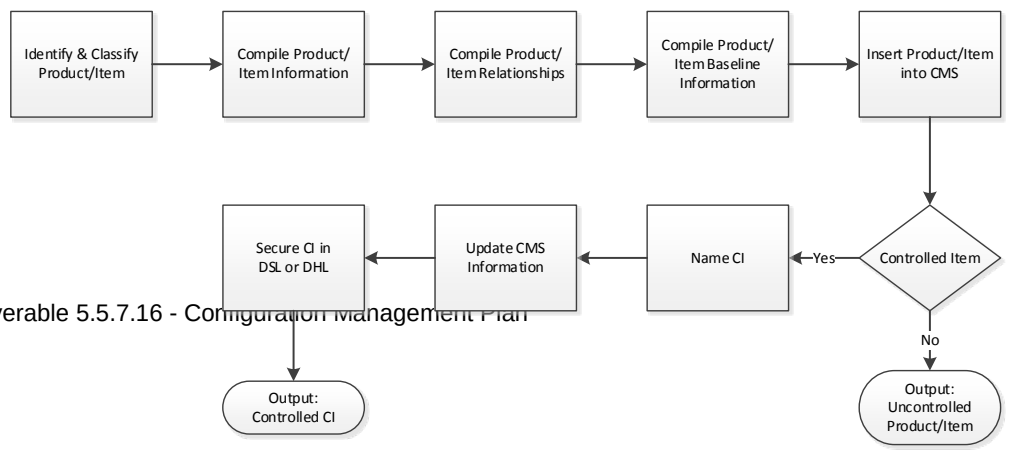
The objective of configuration identification is to create a controllable and auditable list of documented, named, and stored CIs that comprise a controlled environment.

Configuration identification is comprised of three (3) primary activities:

1. Identifying configuration items
2. Naming configuration items
3. Acquiring configuration items

The following diagram reflects the process flow for identifying configuration items.

Figure 23.5.1-1 : Identifying Configuration Items Process Flow



Identifying configuration items

Identifying configuration items is the process of identifying items or products for the controlled environment. A CI is defined as aggregation of work products that is designated for configuration management and treated as a single entity in the configuration management process. The first stage in this process is to classify the item/product into a class or sub class of CIs.

Table 23.5.1.1-1: CI Listing Examples reflects examples of BOS CI.

Table 23.5.1.1-1 : CI Listing Examples

#	CI type	Lower level CI Example
1.	Systems	• BOS-SHOP • BOS-IFP • IVR • XTCM • COGNOS • BOS Reporting Data Store
2.	System Code	• A data file • An executable program • An object module • A source module • A data source ETL file(s)
3.	Environments	• Development • System Integration Test • Performance • Certification • Training • Production
4.	Network	• IP address • Subnet mask • Default gateway • DNS server • WINS server

#	CI type	Lower level CI Example
5.	Physical Hardware	• Data centers • Physical servers • Default gateway
6.	Virtual hardware	• vmWare • memory • network controllers

CI classes are predefined and reviewed semi-annually for continued relevance to a given environment. All changes or additions to the classification definition list must be approved by the Configuration Manager or approved delegate.

Once a CI has been classified, additional item/product attribute information must be obtained for the Configuration Management System (CMS). These attributes must contain a detailed technical and financial description of the item/product for entry into the CMS. Technical details should contain information regarding the item/product capabilities, including where applicable software version or model numbers, hardware specifications, and manufacturer specifications. Additional technical details may be added, as relevant (e.g., networking speeds or data storage size). Hardware technical details should not include items classified as consumables (e.g., desktop keyboards, mice, and cables).

Upon completion of the compilation of the item/product's attributes, the item/product's relationships should be identified and noted. Relationship types will be determined by item/product's classification. In the case of a software classification, all upstream and downstream software dependencies should be identified, as well as which hardware CI(s) are required to support the software. In the event the item/product is a hardware classification, relationships identification should include all supporting hardware required to run the item/product that is currently being evaluated for CM.

Upon completion of identifying the relationships of the item/product, a baseline configuration should be identified and agreed upon by the Configuration Manager or approved delegate and the affected systems development team. A baseline configuration must include everything needed to support the item/product in the agreed upon state for repeatable deployment once the item/product is listed as a CI.

At this stage, the item/product has enough details to be input in the CMS. The BOS CMS is a set of tools and databases that will be used to manage CIs. The CMS includes the use of Microsoft Team Foundation Server (TFS) for collecting, storing, managing, updating, and presenting data about all configuration items and their relationships. The CMS is maintained by the CM Team. At this stage, a determination of whether the item/product is controlled versus uncontrolled will be made. The determination factor for controlled versus uncontrolled is based on whether an item/product will be part of a controlled environment or uncontrolled environment. Controlled environments (certification and production) require full adherence to all governing policies and procedures for Release Management, Change Management, and Configuration Management. Uncontrolled environments, usually prerelease (development, test, or staging) environments, do not require the same level of control, but the

item/products that make up the environment should still be classified as CIs for tracking purposes. No additional steps are required for uncontrolled CIs.

Once a CI has been defined, then other items that may be included as a part of an identified CI can include specifications and interface documents that define the CI.

A CI can also be made up of other CIs. For instance, the certification environment for the BOS would be a CI when the environment is handed over for users to commence the UAT phase. This means that changes to the environment would need to be managed as a part of the CI, which is the certification environment. The certification environment can also contain additional CIs, such as the web portal or the hardware and software that make up the environment, which are also being managed through CM.

Supporting software and systems

The BOS is hosted and supported from several distinct data centers, software applications and systems. For the purposes of CM, each data center is treated as a CI. For instance, the data centers all have elements, which are common to multiple systems in the data center, such as power and networking. In the event these CI elements change, the changes and impacts will be communicated to the Change Control Board (CCB), the operations team and the Exchange. Impacts to a hosting environment will coordinate the necessary changes with other supporting environments and systems in order to prevent impacts to the use of the BOS. These changes can make up a release, which will be tracked through CM.

As a part of the implementation of the BOS into the certification and production environments the environments will come under CM to the extent that they impact the BOS.

23.5.1.1.1. Naming configuration items

Naming configuration items is the process of assigning a unique name to a controlled CI from the approved naming convention. The naming convention, as determined by the Configuration Manager or approved delegate, must allow for multiple versions of the same item/product to be controlled within a controlled environment while maintaining a consistent and repeatable theme for all CIs.

The following tables provide examples of CI naming convention, character values and CI name example.

Table 23.5.1.1.1-1: BOS Code CI Naming Convention

TFS project Name	TFS Branch	Build_Date	Revision	CI Name Example
HIX	DevInt	Core_20130507	3	HIX.DevInt.Core_20130507.3

Table 23.5.1.1.1-2 : CHOICE Server CI Naming convention

Choice Code Character 1-2 *Customer*	Choice Code Character 3-5 *Location / Data Center*	Choice Code Character 6 *Device Type*	Choice Code Character 7-9 *Application Type*	Choice Code Character 10 O/S	Choice Code Character 11 *Status Type*	Choice Code Character 12 *Sequence*	CI Name Example
NV = Nevada	CDC = Converged DC BDC = Backup DC DRBDC = DR BDC IRV = Irvine CA	A = Application B = Backup C = Compute Node D = Database E = E-mail F = Firewall I = IDS N = SAN P = Physical Server R = Router S = Switch V = Virtual Server W = Web Server	BOS = CRM = Customer Relationship Mgmt INI = ININ XTC = XTCM	8 = Windows 2008 L = Linux T = Network Devices U = Unix	D = Development T = Test S = Staging C = Certification E = Training P = Production	01 02 03 04 05 06 07 08 To 99	NVCDCABOS8P01

Table 23.5.1.1.1-3 : Xerox CHOICE Server CI Naming convention

Xerox Code Characters 1-4 denotes the location. (This includes a digit - some cities have more than one data center.)	Xerox Code Characters 5-7 denotes the equipment, OS, and environment	Xerox Code Characters 8-12 (last 2 characters are digits that denotes a server function)	Xerox Code Characters 13-15 denotes the project.	CI Name Example
abc0 def0 gg0	s=server, v=virtual machine, c=cloud os: l=linux, s=solaris	db=database cob=cobol pxy=proxy ftp=ftp	nvh= Nevada HIX	abc0vldpvw01nvh -> Pervasive Worker NV HIX, A

Xerox Code Characters 1-4 denotes the location. (This includes a digit - some cities have more than one data center.)	Xerox Code Characters 5-7 denotes the equipment, OS, and environment	Xerox Code Characters 8-12 (last 2 characters are digits that denotes a server function)	Xerox Code Characters 13-15 denotes the project.	CI Name Example
	environment: p=production, d=development, r=disaster recovery, u=user acceptance testing t=test q=quality assurance s=sit=system integration testing example: slp=server, linux, prod example: vlu=virtual, linux, uat	web=web jbs=jboss wlg=weblogic ctm=control-m apc=apache kid=kidstar oua=online user access jma=job management & admin jas=jasper reports exp=expertpay unv=universe qtz=quartz scheduler wb=web server dm=data management app server dw=data warehouse pvc=pervasive control pvw=pervasive worker cow=cognos web coa=cognos app blz=blaze was=websphere grd=oracle grid		Development Server (ESX VM).

23.5.1.1.2. Acquiring configuration items

Acquiring configuration items is the final activity of the configuration identification process. It involves securing electronic CIs to the Definitive Media Library (DML) or physical CIs to the Definitive Hardware Library (DHL) for storage in the state/configuration agreed upon by the Configuration Manager and the item/product team. It is the responsibility of the Configuration Manager, or approved delegate, to assess each CI to verify its attribute definitions are met and store the CI in the appropriate library, once it is received.

23.5.1.2 Configuration control

Configuration control is the process by which a change to a CI is systematically proposed, evaluated, approved or disapproved, and implemented. It involves three processes, including requesting changes, evaluating changes, and the CCB charter as described in section (23.5.1.5 CCB Charter). Configuration control is an important process for regulating the configuration of system baselines and configuration items and ensuring that only approved changes are implemented. Configuration control validates that system baselines are accurate and known throughout the lifecycle of the CI. Configuration control activities are processed and managed through the CMS. The output of configuration control activities are collected and reported in configuration status accounting and metrics reports.

23.5.1.3 Requesting changes

Requesting changes within CM processes is defined as a request to migrate a CI or group of CIs from one non production environment to another as part of its test cycle, inclusive of a migration or change request to production once it is ready for implementation. The change request (CR) within CM is the process by which a CR is initiated by a requestor for migration or implementation to the certification or production environment. A CR form is to be used for all requests that will be updated throughout the lifecycle of the request and to its disposition. The CR form will include the following items for the CCB evaluation process:

- Request originator
- Class of change (Major, Minor, Emergency)
- CI(s), major components, and interfacing products affected
- Scope and description of change, including work efforts
- Effects on specified performance, operation, maintenance, servicing, operation and maintenance training, spare and repair parts, support and test equipment, and catalogs
- Reason and justification for the change; consequences of not doing the change
- Priority/urgency of the change
- Requested approval date
- Impact Statement
- Rollback Plan (if applicable)
- Change implementation and delivery schedules

Completed CR form(s) will be submitted to the BOS Program CCB for evaluation.

23.5.1.4 Evaluating changes

Evaluating changes is the responsibility of a CCB, which can be made up of a single person or group of people. The BOS will have three (3) CCBs (Refer to Section 23.5.1.5). Each CCB will be constructed to define its area of responsibility and authority to approve or disapprove CRs comprised in a charter. A charter will include measureable and repeatable metrics from which the CCB can derive its decision for a CR. For all CCBs, a chairperson, which will listed as part of the charter, will have the final authority to approve or disapprove a CR.

General determination metrics found within a CCB charter include:

- Is the CR form fully documented?
- Is the CR's risk to business operations acceptable?
- Does the CR violate any contractual or legal obligations?

This evaluation serves as a quality measurement to validate that CIs have been assessed for adherence to the CM processes, impacts to BOS business operations, and alignment to both contractual and legal obligations.

23.5.1.5 CCB Charter

This charter establishes the BOS' three (3) CCBs and assigns responsibility for establishing baselines and controlling changes to CIs within each CCB identified. Three (3) CCBs will be established through the CM process, as follows:

- BOS Program CCB – This is the primary CCB with direct supervision and oversight of the other subordinate CCBs. For any issue that spans multiple CCBs or when a decision deadlock occurs, the BOS Program CCB will review and direct final resolution of unresolved matters.
- Managed Services CCB – This CCB is subordinate to the BOS Program CCB. Its domain of control is over those CIs assigned to Managed Services.
- State Portal CCB – This CCB is subordinate to the BOS Program CCB. Its domain of control is over those CIs assigned to the Web Portal.

Each CCB will operate in an integrated and disciplined manner to provide a structured and streamlined control process for managing the assigned CI throughout their life cycle. Each CCB confirms that all changes are visible, that any potential, security, and operational impacts to the BOS are properly addressed. The CCB provides consistency with technical and programmatic direction across all products and services. The CCB charter empowers each CCB to disposition all changes to these CIs in accordance with the charters designated areas of CCB responsibilities.

CI Assignment

Once CIs have been identified as defined in section 23.5.1.1- Configuration Identification, assignment is conducted by the BOS Program CCB. Transference of CIs between Managed Services and the Web

portal are unlikely however if needed would be directed back to the BOS Program CCB for review and change of classification.

Authority

Each CCB is authorized by the CCB Charter in accordance with the designated areas of responsibilities. This authority extends to the creation of the two (2) lower level CCBs. The charter shall be changed only upon recommendation by the BOS Program CCB.

CCB Responsibilities

The responsibility of the CCB is to assemble the CM team, execute, control, and adhere to the CM plan.

Each CCB will have an Executive Secretary who shall be responsible for ensuring that changes are presented at CCB meetings. The Executive Secretary responsibilities also consist of coordinating and performing the administrative tasks related to the performance of their CCB, including, but not limited to:

- Preparing agenda and formal meeting minutes
- Supporting the change process and procedures (including prescreening, evaluation and resolution of comments)
- Collecting metrics and reporting to each CCB
- Tracking and monitoring CCB action items and Configuration Control Decision (CCD) to closure
- Ensuring that all proposed changes contain security assessment and estimated cost and funding source information. Submitting any unresolved comments to the Chairperson for resolution
- Supporting CM performance monitoring functions, under the authority of this CCB Charter and as described in this plan.
- Ensuring all CM information is validated and entered into the CMS database
- Elevating issues that cannot be resolved within subordinate CCBs to the BOS Program CCB for resolution

CCB Recommendations and Decisions

Each CCB shall review, adjudicate, elevate, or withdraw proposed CRs affecting its CIs or transfer proposed RFCs to other CCBs for adjudication as required. The CCB shall reach a decision after a period of presentation and discussion, at which time the chairperson(s) may poll the members for their position or recommendation. The CCB chairperson(s) shall make all final decisions. CRs may be deferred until the next CCB meeting if further analysis or additional information is needed.

Decisions on CRs shall be documented in a CCD prepared by the CCB Executive Secretary and signed by the CCB chairperson(s). CCD actions will be documented, tracked and monitored through closure within the CMS as part of the CR.

Changes to the CCB Charter

The CCB Charter shall be changed only with the approval of the BOS Program CCB, upon the recommendation of any CCB. CCB Charter change process guidance provides details for establishing an initial charter baseline and maintaining configuration control.

Delegation of CCB Authority

Members of a CCB can delegate their authority. Each CCB chairperson may authorize another CCB participant to act as a chairperson via memorandum to the CCB Executive Secretary. CCB permanent members are responsible for ensuring they are represented at CCB meetings and may delegate specific authority by informing the CCB Chairperson. Additionally, when time critical or urgent processing of a proposed change request is necessary, or in the event of other specific circumstances, the CCB chairperson(s) may call an emergency CCB meeting or approve changes without benefit of a CCB meeting or member review. Change requests processed outside the normal CCB process shall be documented and communicated to permanent members as soon as practical or no later than the next regularly scheduled meeting. Questions and concerns regarding CCB decisions are addressed to the CCB chairperson(s).

23.5.1.6 Configuration Status Accounting

Configuration Status Accounting (CSA) provides information about the current status of approved CIs, as well as the progress and status of proposed and approved changes to the CIs. CSA activities include the collection of data that can be used to measure various aspects of program effectiveness and to assess product completeness and quality.

23.5.1.6.1. Metrics

This section describes what data elements and measures are to be tracked and reported for baselines and changes.

- Date
- CR Identifier
- CI
- Class of Change
- Disposition of CR
    - Pending: New request not reviewed by CCB
    - Disapproved: CCB did not approve CR

- Approved: Ready for RM
- Approved Executed: CR lifecycle completed through RM process
- Approved Rolled Back: Change Rolled Back in RM process

- CR Disposition disapproval reason (if applicable)

Other attributes that will be captured in the Configuration Management database (CMDB) are as follows:

- Technical description
- Financial description
- Capabilities
- Software version or model numbers(if applicable)
- Hardware and manufacturer specification
- Other technical details may be added where relevant:
  - Networking speeds
  - Data storage size
  - Excluding Items classified as consumables. (e.g. Consumables for a desktop would be keyboards, mice and cables)

23.5.1.7 Reporting

This section describes the types of CM status reports that will be generated and their frequencies. Reporting will include data elements and metrics as described in the section above.

Table 23.5.1.7-1 : CI Reporting and Usage

#	Report	Frequency	Purpose	Recipient / Usage
1.	CI Change Report	Weekly	All changed CIs within the reporting period with their current disposition	CM Team The CI Change Report will be used to track approved CIs that are in the process of being changed and its

#	Report	Frequency	Purpose	Recipient / Usage
				readiness to progress its development lifecycle in non-production environments through implementation into production.
2.	CI Inventory Report	Quarterly	All CIs in the program with a summary of total changes to baseline year to date broken out by quarter.	PMO/ Steering Committee A CI inventory will be used as part of report outs for PMO assessment for the level of changes occurring to the BOS system and for communication to the Exchange.
3.	CI Audit Report	Annually	The difference between the actual environment and the latest CI inventory report	CM Team CI differences will be reviewed for quality purposes of maintaining the integrity of changes in all non-production and production environments, based upon the CIs status in its development lifecycle.

23.5.1.8 Configuration Audits and Reviews

Configuration auditing and review is the process of validating the BOS against the CI Inventory Report. The CI Audit Report will be generated to identify any differences. Any items/products found with a difference between the actual and the CIs will be updated in the CMS via CI identification process. If a CI is removed from the BOS, it will be deactivated in the CMS.

The main types of audits conducted on solutions being developed are:

- Documentation configuration audits
- Software and hardware configuration audits

Documentation Configuration Audits

A documentation configuration audit is a systematic and repeatable procedure to verify that the version, date, and location of configured documentation are correct in the project's Document Configuration Items List (DCIL). These audits are conducted on document CIs on a scheduled or as needed basis. A general rule of thumb for these audits is once per quarter and no less than annually.

The goals of a documentation configuration audit are as follows:

- To verify that the project's DCIL information accurately reflects the current documentation on the project's SharePoint sites.
- To confirm that only current, approved versions of documentation are posted on the Xerox document repository (SharePoint).

Software and Hardware Configuration Audits

Configuration audits for software and hardware gather information about the real world, verify and format the data, compare the data to the registered information in the tool, and create a list of the differences. By doing so, it enables an audit of the real world configuration.

Activities may include:

- Performing manual checks within the tools — A manual audit of the CIs entails verifying versioning, CR information, etc. These audits may be performed after each release by selecting a percentage of CIs from the release or a random selection.
- Measuring and reporting the performance configuration audits — The purpose is to measure the effectiveness of improvements to this process.

Triggers for Configuration Audits

Triggers for configuration audits may include the following:

- Requests from defect management or Quality Assurance (QA)
- Verify tool after implementing a CR — After the completion of a change (successful or unsuccessful), this trigger starts the comparing of the relevant real world configuration to the registered information in the tool to analyze the effects of the change and creates a potential list of differences.

23.5.1.9 Access control

Access control to the CMS is role-based, which limits user data availability to the minimum amount of data required to complete their function.

23.5.1.10 Subcontractor/Vendor Control

CM activities will be administered by the team and vendors of subcontractor supplied CIs into the overall BOS. Communication and coordination of changes will be critical to manage the overall health of the solution and prevent unwanted or unknown impacts to the BOS.

For subcontractor developed or acquired items, which are to be incorporated as a CI, the team will:

- Define and describe the new CIs
- Evaluate the expected impact of the CI to the overall configuration management of the system
- Define the rolls and expected participation of the subcontractor as it applies to CM
- Define the long term CM impacts of the subcontractor
- Define the exit strategy of the subcontractor from the overall CM process
- Communication of known schedule
- Communication of expected delivery
- Communication of known CM processes
- Communication of expected participation in CM

23.5.1.11 Subcontractor requirements matrix

Subcontractors are expected to adhere to all CM requirements for which the team requires the subcontractor to participate.

23.5.1.12 Compliance monitoring

The Exchange requires active subcontractor participation in status reporting and reviews of subcontractor CIs. Depending on the CIs, compliance monitoring will be defined by the PMP, as well as overall participation of the subcontractor in required CM processes.

23.5.1.13 Evaluations and reviews

Depending on the subcontractor CIs, reviews may include incorporation of the CIs into an existing non-production environment for initial evaluation and review. The overall process for such a review would follow the Release Management Plan. Detailed project schedules and timelines will be provided to subcontractors, which will specify necessary configuration evaluations and reviews.

23.5.1.14 Incorporation

Incorporation of new subcontractor CIs into the CM process will follow processes documented in the Release Management Plan. This means that the CIs will be implemented into each applicable environment where they are tested, verified, accepted, and merged to the BOS, as appropriate.

23.5.1.15 Intellectual property

Intellectual property can be defined as a part of the contract with a subcontractor entity or as a part of a software license agreement, depending on the CI.

23.5.1.16 Change Management

Changes are managed per the deliverable 5.4.3.4.C – 22 Change Management Plan, located in the BOS project SharePoint site.

23.5.1.17 Acquired software

Acquired software will follow the Release Management Plan and this CM Plan, just like any other CI. Participation from a software supplier will be dependent on the CI and will be defined by project management.

23.5.1.18 Release Management and Delivery

Release management and delivery are managed per the Release Management Plan, Chapter 12 of the PMP.

23.5.2 CM Schedule

This section reflects schedule information for the sequence and coordination of CM, its' activities and frequency.

Key dependencies to activities reflected in Table 23.5.2-1: CM Activity Schedule are :

- Execution and adherence to change management processes such as identification, analysis and approvals of formal CRs.
- Execution and adherence to release management processes such as creation of RM artifacts and controls of releases, and all interrelated system dependencies.
- Execution of CM activities and management of code changes for build labeling and use of CMS tools for code storage and propagation for testing and implementation.
- Execution and adherence to activities that would define necessary changes through activities as described in the other core plans including the Support and Problem Escalation Plan; the Service Management Process; the Data Retention, Recovery Services, Protection and Data Management Plan; and the Hosting Environment Plan.

Table 23.5.2-2 : CM Activity Schedule

CM Activity	Frequency
Plan CM activities and resources	At program startup/ongoing
Provide Weekly Status Report	Weekly

CM Activity	Frequency
Report CM activities to management	Monthly
Develop CM Plan	At program startup/ongoing
Operationalize CM Plan	Upon approval for CM plan
Establish and maintain CM Library	At program startup/ongoing
Archive CM records	At selected milestones and at close of project
Conduct CM Training	As needed
Configuration Identification	**Frequency**
Configuration Item Identification	At program startup/ongoing
Configuration Item Selection	At program startup/ongoing
Maintain Configuration Item List	Ongoing
Establish Baselines	At defined milestones
Update Baselines	Ongoing (or as needed)
Create Software Builds	TBD based upon release schedules
Change Control	**Frequency**
Manage Changes, Change Requests	Ongoing
Conduct CCB Meetings	Monthly (or as needed)
Configuration Status Accounting	**Frequency**
Collect Configuration Status Accounting information	Ongoing, at specified schedules
Prepare Configuration Status Accounting	Ongoing

CM Activity	Frequency
reports	
Collect Metrics	Monthly
Prepare Metrics reports	Monthly
Configuration Audits and Reviews	**Frequency**
Conduct Unscheduled Baseline Audits	As Required (at minimum bi annually)
Conduct scheduled audits	At defined milestones (may be scheduled quarterly dependent a particular release development cycle)

23.5.2.1 Milestones

This section identifies project milestones related to the approval, training, and monitoring of CM. The milestones listed below must be included in the project schedule:

- The CM Plan is approved by the PMO
- The CM Plan is approved by the Exchange
- The CM Team is established
- Project staff are oriented and trained on CM processes

23.5.2.2 Verification Steps

Verification steps are tasks or oversight processes executed to confirm that the approach detailed in this document is adhered to throughout the project.

Table 23.5.2.2-1: Verification Steps

Verification Steps	Frequency
The PMO and BOS leads CI reviews against the Configuration Management Plan	At least yearly
PMO reviews the Configuration Management Plan	At least yearly

23.5.3 CM Resources

This section describes CM roles and responsibilities, infrastructure, tools, methods, standards, techniques, and training necessary for implementing CM processes.

23.5.3.1 Roles and Responsibilities

To validate completion of activities and processes in this plan, responsibilities must be assumed by one or more individuals on the project. The project manager or resource manager determines how responsibilities are allocated to project resources.

The following table identifies the roles and responsibilities related to the CM Plan.

Table 23.5.3.1-1: Release Management Roles and Responsibilities

#	*Role*	*Description*
1.	Configuration Manager	Coordinates with the project team and the Release Management Team to confirm adherence to the overall Configuration Management process. This role functions as a team member of the Configuration Management team.
2.	Configuration Control Board	The CCB will : • Review recommendations to change the configuration of the BOS • Monitor the development and implementation of improvements • Coordinate with BOS stakeholders to confirm recommended system changes are not counterproductive regarding modernization policy or process • Ensure complete, accurate, and timely changes are made to configuration documentation This role functions as a team member of the Configuration Management team.
3.	Change Control Management	Change Control Management (CCM) are staff responsible for entering submitted CRs, preparing change control documents, and providing each CR requestor status on their request entered into the change request tracking tool.

#	Role	Description
		This role functions as a team member of the Change Management team.
4.	Configuration Management Team	The CM Team is responsible for promoting and migrating code through the BOS environments (i.e., system integration testing, user acceptance testing, and production)
5.	Release Management Board	The Release Management Board (RMB) is responsible for making decisions on the priority of releases based on various dependencies and risks. This role functions as a team member of the Release Management team.
6.	Release Management Team	The RM Team is responsible for analyzing and prioritizing release requests in support of the Steering Committee. The RM Team verifies that the impacts and rationale for changes to CIs are analyzed and coordinated prior to being released to the controlled environments.
7.	Test Manager	The Test Manager confirms that scheduled releases are fully tested; the CRs meet customer expectations, and verify that IT operations are able to support the changes. This role functions as a team member of the project and participates as a contributing member of release, configuration teams.
8.	BOS System Leads	BOS System Leads own the following tasks: • Manages source code and migration of application code through the various environments • Creates Project Release Plan identifying all CIs related to a CR • Deploys code to respective environments • Updates configuration settings • Works closely with Configuration and Release Analyst to communicate changes required when moving from one environment to another • Participates in and provides input to Configuration Meetings This role functions as a team member of the project and participates as a contributing member of change, release, and configuration management

#	Role	Description
		teams.
9.	Change Management Team	The team of individuals and staff which make up the implementation of the Change Management Plan, including: • Change Request Identifier/Owner • PMO (CR Coordinator) • Project Manager(s) / Steering Committee • Executive Sponsors • Exchange Project Manager • Xerox Project Manager • Project Staff Please refer to deliverable 5.4.3.4.C – 22 Change Management Plan
10.	Steering Committee	The Steering Committee approves releases for release into the production environment (prior to the release date). The Steering Committee is made up of designated Exchange representatives including executive management of the Exchange.
11.	Change Control Coordinator	The PMO/Change Coordinator controls the life cycle of all changes from receipt of a change until approval/rejection is received. The primary objective is to enable beneficial changes to be made, with the minimum disruption to an IT service. For important changes, the Change Coordinator will defer the authorization of changes to the PMO & Change Management Team. This role functions as a team member of the Change Management Team.
12.	Test Team	The primary role of the Test Team is to complete and confirm proper testing for the releases prior to implementation.
13.	External partners	DWSS or other external partners who participate in appropriate release planning meetings, may review test cases, and may provide approval to deploy each release into production, based upon affecting changes. This role functions in as an external team member of the project and participates as a contributing member of the release and configuration

#	Role	Description
		teams as needed.

23.5.3.2 Applicable Tools and Methods

Table 23.5.3.2-1: Applicable Tools and Methods Table

#	Tool/Method	Description
1.	Microsoft Team Foundation Server	Version control, for managing source code and other deliverables that require versioning. Work item tracking, for keeping track of such things as change requests, defects, requirements, tasks, and scenarios. Project management functions and reporting, which enable project planning and reporting, managing resources and assigning responsible parties, percentage complete, history and dependencies.
2.	Change Control Log	A Microsoft SharePoint database (list) will be used to capture/reference document detail about each change request, including the decision related to each change request.
3.	BMC FootPrints	BMC FootPrints is the CMS software, which will be the point of authority for all request for changes and change requests.
4.	Rational ClearCase (UCM)	Rational ClearCase is used by the team as source code repository, configuration control tool. Builds and release streams are used for version releases. Build and release scripts (shell scripts) are used to promote the releases to various environments.
5.	Rational ClearQuest	Used by team to manage change control. UCM allows ClearQuest to integrate with Clearcase to enforce defect and change tracking with code development through the use of activities
6.	IBM DOORS	The requirements traceability database that will be used by the Exchange teams to track requirements and produce an initial, subsequent requirements traceability matrices, and subsequent change requests.

23.5.3.3 Applicable Standards

The following section identifies the applicable standard applied to the configuration management process for the BOS.

- **IEEE Std 828 - 2012 IEEE Standard for Configuration Management in Systems and Engineering** – This standard establishes the minimum requirements for processes for CM in systems and software engineering. The application of this standard applies to any form, class, or type of software or system. This revision of the standard expands the previous version to explain CM, including identifying and acquiring configuration items, controlling changes, reporting the status of configuration items, as well as software builds and release engineering. Its predecessor defined only the contents of a software configuration management plan. This standard addresses what CM activities are to be done, when they are to happen in the life cycle, and what planning and resources are required. It also describes the content areas for a CM Plan.

23.5.3.4 Infrastructure

The CM Plan is supported by the software and hardware defined within the BOS data centers, as described in deliverable 5.5.7.2 Hosting Environment Plan, located in the BOS project SharePoint site.

23.5.3.5 Training

Project team members are trained in the duties and responsibilities of CM. As new members are added, they receive comparable training, as needed. The PMO supports the training of members who will receive at least one of the following:

- Project Control training, which includes training in Change Control, Configuration and Release Management
- Configuration management tool and process training
- Release migration training

23.5.4 CM Plan Maintenance

The purpose of creating a CM Plan is to methodically track and document changes so that systems and CIs maintain their integrity over time. A database, tool, or tracking document would act as an historical record of changes to applications and CIs and would maintain a “snap-shot” of the environment. The database, tool, or tracking document can contain the components of an application and its version, or a repository with the current status and location of documents. It provides an organized view of the applications and CIs and a means to track and control them. The Xerox SharePoint is the repository that is used to store and manage document CIs within the Document CI List.

Specific activities help retain knowledge about CIs and institute strategies for staying informed about changes that influence CIs. Some of these activities include:

- Gathering and reviewing upcoming changes — CM utilizes the Change Control Management Plan as part of the configuration framework. The Change Control Management Plan details how changes to items are conducted, which include use of the ClearQuest tool, change log, and CCB for change review, approvals, and denials.

- Assessing the impact of a change – Each identified change can potentially require an update to the database, tool, or tracking document.

23.5.4.1 Triggers for CI Planning and Maintenance

Triggers for planning and maintenance of the CIs may include the following:

- New CR (each change has to be evaluated)
- Changes in the infrastructure design
- Changed Service Level Agreement (SLA)
- Problem and defect management (each incident has to be evaluated)
- CR — The configuration changes resulting from an authorized change have to be registered into the tool, if successfully implemented. This includes Problem and Defect management changes.
- Identified differences — After each audit of the configuration, the differences are evaluated and can result in updates of the tool.

23.5.4.2 Managing Configuration Items

The project manager, working with the project team, verifies the BOS deliverables, manuals, and development artifacts are managed as defined in the Document Configuration Items List. The project manager includes status information related to the CM in the project's weekly status report, as appropriate.

The project manager confirms that developed BOS systems and test software source code will be placed under the control of a software CM system. Refer to the Applicable Methods and Tools section (Section 23.5.3.2) of this document for a list of software CM tools.

In addition, the project manager verifies that changes to CIs are managed as defined in the tool, assuring timely and accurate information is provided to appropriate stakeholders.

Activities for managing CIs may include the following:

- Identifying authorized changes to the infrastructure (real world) — Changes will be done based on a CR that has gone through the change management process and has been authorized. This activity identifies these changes and prepares them to be applied to the administered configuration in the RM and CM tools.
- Identifying a list of preauthorized types of changes — There are defect changes that do not go through the standard change management process, but are still to be administered in the RM and CM tools. An example may be an emergency or bug fixes which are controlled in the release management process.
- Validating changes (naming convention, completeness, etc.) — Authorized changes are validated on their completeness and compliance with the project policies (e.g., peer review of code). This activity also validates the completeness of documentation requirements and confirms that the owners of each CI are known.

- Updating the approved changes into the tool — This activity updates the actual entries based on the authorized changes.
- Creating relationships between CIs —This activity uses the change management process and checks against standard configurations to determine the relationships a CI has with other CIs.
- Creating a soft label or tag — Each CI will be marked with a unique label or tag. The soft label is not only unique for a CI, but also unique for different versions, or configurations, of a CI. This way the various configurations of a CI can be traced through its life cycle.
- Signaling to defect management — This activity takes an audit list to verify if each difference is based on an authorized change or a preauthorized change.

23.5.4.3 Monitoring

The PMO maintains responsibility for the CM Plan and monitoring its output for validity and alignment with operational procedures.

23.5.4.4 Update Frequency

The CM Plan is to be reviewed by the BOS Program CCB at least annually or as frequently as deemed necessary by the BOS Program CCB for continued validity and alignment with operational procedures.

23.5.4.5 Change Approval

The CM Plan changes will follow the established policies and procedures contained within this document for approval. Only the PMO has the authority to approve a change to the CM Plan.

23.5.4.6 Change Control & Communication

The CM Plan change control and communication will follow the established policies and procedures contained within deliverable 5.4.3.4 C Change Management Plan, located on the projects SharePoint site.